Testimony of

Christopher Koch

President & CEO of the

World Shipping Council

Regarding

Maritime and Port Security

Before the

Senate Committee on Commerce, Science, and Transportation

February 28, 2006

Introduction

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association representing international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93% of the United States' imports and exports transported by the international liner shipping industry, or more than $500 billion worth of American foreign commerce per year.[1]

I also serve as Chairman of the Department of Homeland Security's National Maritime Security Advisory Committee, as a member of the Departments of Homeland

[1] A list of the Council's members can be found on the Council's website at www.worldshipping.org.

Security's and Treasury's Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Council. It is a pleasure to be here today.

In 2005, American businesses imported roughly 11 million loaded cargo containers into the United States. The liner shipping industry transports on average about $1.5 billion worth of containerized goods through U.S. ports each day. In 2006, at projected trade growth rates, the industry will handle roughly 12 million U.S. import container loads. And these trade growth trends are expected to continue after 2006.

The demands on all parties in the transportation sector to handle these large cargo volumes efficiently is both a major challenge and very important to the American economy.

At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to enhance maritime security, and do so in a way that doesn't unreasonably hamper commerce.

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

What is the appropriate collection of measures to address this challenge?

The Department of Homeland Security's maritime security strategy involves many different, but complementary, pieces.

It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and the Maritime Transportation Security Act (MTSA).

It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code.

It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one.

The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area.

And last, but certainly not least, these directives and efforts include an array of initiatives to enhance *cargo security*, including

- Cargo Security Risk Assessment Screening
- The Container Security Initiative
- The C-TPAT Program
- Container Inspection Technology Deployment

The liner shipping industry and the members of the World Shipping Council have fully supported these various initiatives. Ocean carriers' business depends upon the government having a security regime that provides adequate levels of security confidence, while continuing to allow for the efficient and reliable transportation of America's exports and imports.

The government's multi-layer security strategy is a fundamentally sound one, and seeks to address cargo and maritime security on an international basis as early as is practicable. It does not wait to address security questions for the first time when a ship and its cargo arrives at a U.S. port. The strategy can be further developed and strengthened, however, and we appreciate the Committee's continued interest in these issues. The following is a brief description of the strategy's various layers.

1. Vessel Security

Every vessel entering a U.S. port, whether of U.S. or foreign registry, has a ship security plan that is in accordance with the ISPS Code – a binding international convention developed under the leadership of the U.S. Coast Guard. The Coast Guard also ensures through its port state enforcement programs that vessels entering U.S. ports are in compliance with the Code. Vessels that are not in compliance are denied entry into a U.S. port by the Coast Guard.

Under MTSA, the Coast Guard requires vessels to file advance Notice of Arrivals 96 hours before arrival in a U.S port, providing relevant advance information about the vessel, its itinerary, its crew and its cargo. The Coast Guard and Customs and Border Protection (CBP) use this information for risk profiling.

2. Port Security

Port facilities must also comply with the ISPS Code, and, in the U.S., the Coast Guard's MTSA regulations – the regulatory regime used to implement the ISPS Code domestically. All major U.S. ports are in compliance with the ISPS Code.[2]

These port facilities or marine terminals may be operated by the state or local government public port authority, or they may be leased from the port authority by terminal operating service providers, with the port authority maintaining ownership and oversight of the port. The majority of U.S marine terminals are operated by private marine terminal firms, who have leased the property from the port authority. Major ports generally have multiple terminals and terminal operators.

Stevedoring and marine terminal operations are a service industry that is open to foreign investment. Billions of dollars of foreign investment has been made in the U.S. over recent years in this sector, and that investment has contributed substantially to a transportation infrastructure that is critical to moving America's commerce efficiently and reliably. The investment has come from Japanese, Korean, Danish, British, Chinese, French, Taiwanese, and Singaporean businesses, just as American companies have been allowed to invest in marine terminal and stevedoring businesses in foreign countries.

The substantial majority of American containerized commerce is handled in U.S. ports by marine terminal operators that are subsidiaries or affiliates of foreign enterprises. This is an international, highly competitive industry, providing hundreds of thousands of American jobs. The United States depends on it, and it in turn has served the needs of American commerce well, adding capacity and service as the needs of American exporters and importers have grown.

An important element of the U.S. government's position in international trade negotiations for many years, under both Democrat and Republican administrations, has been the importance of securing the ability of international investment to flow into various international service industries. It is a principle of substantial importance to many sectors of the American economy.

Port facilities, such as the ones operated by P&O Ports and to be purchased by DP World Ports, must and do comply with all the government's applicable security requirements. There is no evidence that terminal facilities' operations conducted by foreign controlled companies are any less secure, or in any way less compliant with security regulations, or in any way less cooperative with U.S. government security authorities than U.S. controlled companies. In fact, these companies work closely and cooperatively with the Coast Guard, Customs and Border Protection, the U.S. military, and other U.S. law enforcement agencies.

[2] The Coast Guard's MTSA regulations estimated that the industry's compliance with the Code would cost more than $8 billion over ten years, and that figure did not include foreign port or foreign vessel compliance costs.

The World Shipping Council and its member carriers are committed to the effective implementation of port security requirements around the world. In this regard, the Council and its member lines are in the final stages of establishing a cooperative program with the U.S. Coast Guard pursuant to which the industry's member lines may report port facility security status issues to the Coast Guard in order to assist with that agency's global maritime security efforts.

3. Personnel Security

Maritime personnel security is addressed in various ways. Vessels must provide CBP and the Coast Guard with advance notice of all crew on the vessel 96 hours before the vessel arrives in a U.S port for screening. U.S. seafarers are issued credentials by the U.S. Coast Guard and must go through a security vetting process. All foreign seafarers must have valid, individual U.S. visas if they are to go ashore while in the U.S.

Regarding personnel working in U.S. ports, the Department of Homeland Security has indicated that it intends to promulgate proposed rules on the Transportation Worker Identification Credential (TWIC) in the near future, as required by MTSA. At the request of DHS, the National Maritime Security Advisory Committee, after intensive, open and constructive dialogue amongst diverse industry and government officials, approved a detailed set of recommendations to the Department for their consideration in the development of this initiative. The establishment of the TWIC should help meet one of the unaddressed U.S. port security imperatives identified by Congress and DHS as an essential element of the nation's maritime security. The Council and its Member lines strongly support DHS promulgating a regulation on this issue.

4. Cargo Security

Particularly with respect to containerized cargo, the issues surrounding cargo security are challenges that require a multi-faceted strategy, which begins long before the cargo arrives at a U.S. port. It involves advance Customs security screening of all containers before vessel loading in the foreign port, cooperation with foreign Customs authorities through the Container Security Initiative, use of container inspection technology, and the Customs Trade Partnership Against Terrorism initiative.

a. Risk Assessment and the National Targeting Center

The stated and statutorily mandated strategy of the U.S. government is to conduct a security screening of containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The World Shipping Council fully supports this strategy. The correct time and place for the cargo security screening is before the containers are loaded on a ship. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments aboard a vessel put at risk or delayed because of a security concern that could arise regarding another cargo shipment aboard the ship.

In order to be able to perform this advance security screening, CBP implemented the "24 Hour Rule" in early 2003, under which ocean carriers are required to provide CBP with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. The Council supports this rule. CBP, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without further review. Every container shipment loaded on a vessel bound for the U.S. is screened through this system before vessel loading at the foreign port. Customs may issue the carrier a "Do Not Load" message on any container that is so screened if it has security concerns that need to be addressed.

The Department of Homeland Security's strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100% of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100% of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5-6% of all inbound containers (over 500,000 containers/year), using either X-ray or gamma ray technology (or both) or by physical devanning of the container.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo shipment have been addressed prior to a vessel being loaded and sailing. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to CBP for each shipment for the before-vessel-loading security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers' manifest data has limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities.[3] *Currently, there is no data that is required to be filed into ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process*. This occurs, even though these parties possess shipment data that government officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to

[3] *See also,* "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", General Accounting Office Report and Testimony. March 31, 2004 (GAO-04-557T).

loading in a foreign port"[4]. Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until after the cargo shipment is in the United States, often at its inland destination – too late to be used for security screening purposes.

In September 2004, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide CBP with the following data before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check.), and
9. Origin of container shipment – the name and address of the business where the container was stuffed, which is often not available from an ocean carrier's bill of lading.

The Council agrees with this recommendation. The government's strategy today is to inspect containerized cargo on a risk-assessment basis. Accordingly, the government should improve the cargo shipment data it currently uses for its risk assessment. An ocean carrier's bill of lading by itself is not sufficient for cargo security screening. Earlier filing of these shipment data elements would improve CBP's cargo security screening capabilities. If a risk assessment strategy is to remain the core of the government's cargo security system, the government needs to decide what additional advance cargo shipment information it needs to do the job well, and it must require cargo interests, and not just carriers, to provide the relevant data in time to do the advance security screening. While this is not a simple task, a next step forward requiring shipper interests to provide more data on their cargo shipments before vessel loading is appropriate.

I would like to note and commend the Committee Chairman, Senator Stevens, and the eleven other Senators cosponsoring S. 1052, for their inclusion in that bill of a requirement that importers provide CBP with such advance customs entry information for security screening purposes before vessel loading, just as carriers provide the information they have before vessel loading.

CBP and DHS officials are currently reviewing this issue.

[4] 46 U.S.C section 70116(b)(1). Section 343(a) of the Trade Act also requires that cargo information be provided by the party with the most direct knowledge of the information.

b. Container Security Initiative

No nation by itself can protect international trade. International cooperation is essential. For ships and port facilities, the International Maritime Organization (IMO), a U.N. regulatory agency with international requirement setting authority, has responded to U.S. leadership and created the International Ship and Port Security Code (ISPS). These IMO rules are internationally applicable and are strictly enforced by the U.S. Coast Guard. There is no comparable international regulatory institution with rule writing authority for international supply chain security. For a variety of reasons, the World Customs Organization (WCO) has not acquired such an authority.

At the WCO, CBP continues to work diligently with other governments on a supply chain security framework that can be used by all trading nations. This framework will be useful, but will remain at a fairly high level and will be implemented on a voluntary basis by interested governments. Consequently, U.S. and foreign customs authorities must also create a network of bilateral cooperative relationships to share information and to enhance trade security. This is the Container Security Initiative. The Council fully supports this program and the strategy behind it.

Today, 72% of U.S. containerized imports passes through 42 operational CSI ports (including Dubai, which became a CSI participant in March 2005), with further program growth expected. CBP hopes to expand the CSI program to 50 ports by the end of this year, which could cover roughly 85% of U.S containerized imports.

The liner shipping industry is fully supportive of these efforts by CBP authorities and hopes the program will continue to expand as expeditiously as possible. A listing of operational CSI ports follows:

Port Name	**2004 US Imports TEUs (000)**
Yantian (Shenzhen)	1,982.79
Hong Kong	1,866.32
Shanghai	1,278.50
Kaohsiung	1,127.27
Busan	971.49
Singapore	494.30
Rotterdam	427.75
Bremerhaven	392.18
Antwerp	304.60
Tokyo	267.53
Laem Chabang	201.06
Nagoya	174.94
Le Spezia	159.67
Hamburg	150.01
Santos	146.26
Genoa	144.57
Le Havre	139.67

Kobe	119.97
Colombo	117.08
Yokohama	109.02
Gioia Tauro	104.48
Livorno (Leghorn)	92.33
Algeciras	81.75
Felixstowe	69.51
Buenos Aires	52.40
Tanjung Pelepas	45.96
Durban	43.94
Liverpool	39.37
Port Kelang	39.26
Southampton	38.62
Thamesport	32.34
Naples	29.88
Lisbon	26.91
Halifax	24.38
Gothenberg	18.81
Vancouver	13.59
Piraeus	11.58
Tilbury	2.56
Dubai	1.11
Marseille	1.07
Montreal	0.72
Zeebrugge	0.02
Total CSI Ports	*11,344.55*
Non-CSI Ports	*4,460.93*
Total All Ports	*15,805.48*

c. C-TPAT

Customs' Trade Partnership Against Terrorism (C-TPAT) is an initiative intended to increase supply chain security through voluntary, non-regulatory agreements with various industry sectors. Its primary focus is on the participation of U.S. importers, who are in turn urged to have their suppliers implement security measures all the way down their supply chains to the origin of the goods. This approach has an obvious attraction in the fact that the importer's suppliers in foreign countries are beyond the reach of U.S regulatory jurisdiction. In return for participating in the program, importers are given a benefit of reduced cargo inspection. The C-TPAT program invites participation from other parties involved in the supply chain as well, including carriers, customs brokers, freight forwarders, U.S. port facilities, and a limited application to foreign manufacturers.

CBP has been working to strengthen the C-TPAT program and to increase validations of participants' performance. C-TPAT is not a regulatory program, and it is not a guarantee of security. It does, however, provide for a creative partnership approach between government and industry as one element of a multi-layered strategy to improve security. It clearly has value, even though it can't be easily measured or quantified; and,

because its principal purpose is to try to affect the conduct of parties outside U.S. regulatory jurisdiction, it has a reach that regulations alone could not have.

Many maritime and supply chains security issues can be, should be, and are addressed through regulatory requirements, not C-TPAT. For example, vessel security plans and port security plans are regulated by Coast Guard regulations implementing the ISPS Code and MTSA. The data that must be filed with CBP to facilitate cargo security screening must be addressed through uniformly applied regulations. Seafarer credentials and the Transportation Worker Identification Card must be addressed through uniformly applied requirements.

C-TPAT, however, is a program that can try to address matters that are not or cannot be addressed by regulations, such as supply chain enhancements beyond U.S. regulatory jurisdiction, or matters that aren't covered by regulations.

d. Container Inspection Technologies

Technology clearly has a role in increasing both the efficiency of inspecting containerized cargo shipments and the number of containers that could be inspected. Container inspection technology is of substantial interest because -- unlike so many other technologies –it helps address the container security question of paramount importance, namely: "What's in the box?"

X-ray and gamma ray non-intrusive container inspection (NII) equipment is being deployed at U.S. and foreign ports. At U.S ports, CBP has deployed 170 large scale non-intrusive inspection devices. NII inspection equipment allows Customs authorities to have a visual image of a container's contents, is a relatively easy way to review a container's contents in contrast to physically devanning the container, and is usually adequate for inspecting a container considered to be of security interest.

A particular security concern is the potential use of a container to transport a nuclear or radiological device. While there is no evidence that terrorists have nuclear weapons or devices, or that a shipping container would be a likely means to deliver such a device, the consequences of the potential threat -- including those from a low-tech "dirty bomb"-- are sufficiently great that, in addition to the targeted inspection of containers discussed above, CBP is deploying radiation scanning equipment at all major U.S container ports. CBP has deployed between 180-190 radiation portal monitors at U.S. ports and we understand that these presently cover approximately 37% of the imported containers. CBP has also deployed thousands of hand-held radiation detection devices. CBP and the Department of Energy are also working with foreign ports to install radiation scanning technology abroad as well. Availability of such technology is one of the criteria that a foreign port must meet to become a CSI port, for example.

Container inspection technology may be evolving to the point that it may be deployed in the foreseeable future to allow radiation and NII inspection of all containers entering a port facility without significant delay to commerce. If this were to prove true,

and if the radiation and image readings are of sufficient quality for security screening purposes, this capability would allow a new and significantly more effective supply chain security strategy to be deployed. Such capability could enable governments to "flex" their security screening capabilities, to inspect more containers, even from a remote location, without having to inconvenience terminal operators or other customs authorities, and to more effectively handle a response to a transportation security initiative, including the NII inspection of every container being loaded at a particular port, if needed. Such a capability would also have the advantage of being able to inspect more containers before vessel loading, rather than waiting until they arrive in the United States discharge port.

CBP and DHS officials are presently reviewing this technology and the pilot application of radiation-NII inspection technology to all containers entering two different Hong Kong port facilities. The technology is conceptually attractive, but a real world evaluation of the technology, its effect on operations, and its integration into and use by the government is clearly needed. For example, numerous nuisance alarms are likely to occur on a daily basis, and there will need to be clear protocols for how such situations will be addressed and resolved in the foreign ports. Other operational issues need to be clearly understood and addressed, including how such technology might be applied at transshipment ports, where cargo does not arrive through a terminal gate. While it is true that under this pilot program containers entering the truck gates of two Hong Kong container terminals have passed through these scanning and radiation detection devices, no one is actually using the Hong Kong pilot container inspection readings or images, or transmitting them to Customs, or applying the results of the technology in the operating environment. We are at the beginning stages of working through the issues involved, including determining whether and how CBP would like to embrace this technology.

If the government determines that the technology works satisfactorily, it will be necessary to determine how the information produced by this technology would be transferred to the government and used and analyzed, and by whom and when. In addition, the technology obviously must be physically sited on marine terminals around the world. This would be a challenge, but may be possible if the proper foundation is negotiated and laid with foreign governments and terminal operators and provided the correct incentives are established. This will require addressing roles and responsibilities, substantial data transfer protocols, and issues of liability.

It is also relevant to note that this kind of system would be impossible to deploy without the full cooperation and agreement of foreign terminal operating companies and their governments. It is also relevant to note that global application of this technology would almost certainly involve its installation and application at U.S. ports to U.S. export cargo, and sharing the resultant data with other interested foreign governments.

There are significant and legitimate issues that need to be addressed in considering this technology and its possible deployment; however, the capability for governments to call up and review radiation and NII images of any container before vessel loading without delaying commerce could potentially provide a significant improvement in security capabilities. Furthermore, it could allow governments the

flexibility to change their container security strategies in a way that would provide increased security assurance for all legitimate commerce, including the capacity to provide sufficient assurance of security to keep commerce flowing in the event of a container security incident.

Summary

When addressing the issue of international maritime security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization of the world economy, the remarkable growth of world trade, and the U.S. economy's appetite for imports – a demand that fills our ships, our ports, and our inland transportation infrastructure, a demand that produced more than 11 million U.S. import containers in 2005, and will produce roughly 12 million this year, and a demand that will increasingly test our ability to move America's commerce as efficiently as we have in the past.

The other dynamic is the threat to our way of life from terrorists and the challenge of addressing the vulnerabilities that exist in the free flow of international trade, even when the specific risk is elusive or impossible to identify.

Finding the correct, reasonable balance between prudent security measures and overreacting in a way that impairs commerce is a tough challenge.

Foreign equity in the international maritime transportation business is not the security challenge. It has been and continues to be a major, long-standing and positive contributor to an infrastructure that is essential to the American economy and to U.S. national security, and its interest in ensuring the safety and security of maritime commerce is very strong. After all, without a reliable, secure and efficient maritime transportation system, these companies' businesses are in jeopardy.

The maritime security challenge is to build on the fundamentally sound strategic framework that DHS has developed and to continue to make improvements on what has been started. Specifically, we believe that priority DHS consideration should be given to:

1. Improving the cargo shipment data collected and analyzed by CBP's National Targeting Center before vessel loading. If cargo risk assessment is to be a cornerstone of DHS policy -- which we believe is a correct approach, and cargo security screening is to be performed before the cargo is loaded onto a ship destined for the U.S. -- which we also believe is a correct approach, it should be using more complete cargo shipment data to perform the risk assessment than only the ocean carriers' bills of lading;

2. Expanding international cooperation through the Container Security Initiative network;

3. Continuing to improve and strengthen the C-TPAT program;

4. Promulgating regulations to implement the MTSA mandate of maritime Transportation Worker Identification Cards; and

5. Undertake a close examination of the merits and feasibility of widespread application of ICIS-type X-ray inspection and radiation screening equipment and the interface and use of such equipment by Customs authorities. While not a simple issue, this might hold the potential to significantly improve governments' confidence in the security of importers' and exporters' cargo shipments.

Mr. Chairman, the World Shipping Council and its member companies believe that there is no task more important than helping the government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We are pleased to offer the Committee our views and assistance in this effort.